UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/734,817	12/12/2003	Bernard D. Aboba	13768.432.1	3500

47973 7590 02/06/2009
WORKMAN NYDEGGER/MICROSOFT
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UT 84111

EXAMINER	
JOHNSON, CARLTON	
ART UNIT	PAPER NUMBER
2436	
MAIL DATE	DELIVERY MODE
02/06/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/734,817	**Applicant(s)** ABOBA ET AL.	
	Examiner CARLTON V. JOHNSON	**Art Unit** 2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11-11-2008*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28,41 and 42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28,41 and 42* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application
6) □ Other: _____.

DETAILED ACTION

1. This action is responding to application amendments filed on 11-11-2008.

2. Claims **1 - 28, 41, 42** are pending. Claims **1, 10, 19, 24, 41** have been amended. Claims **29 - 40, 43** have been cancelled. Claims **1, 10, 19, 24, 41** are independent. This application was filed on 12-12-2003.

Response to Arguments

3. Applicant's arguments filed 11-11-2008 have been fully considered and were not persuasive.

3.1 Applicant argues that the referenced prior art does not disclose, the concept to verify discovery information at an access point and a discovery verification request includes at least part of the discovery information obtained from an access point. (see Remarks Pages 9-11)

The Whelan prior art discloses the discovery of identification information concerning an access point and a verification process in order to verify an access point. The Whelan prior art discloses a verification process for the discovered information concerning an access point. The Whelan prior art does not discredit or discourage other discovery (and verification) processes (see Whelan paragraph [0053], lines 5-6: discovery (and authentication) process can use any suitable method), therefore the Whelan prior art does not teach away from a verification process such as taught by the Meier prior art which contacts an access point for verification. (MPEP 2145[R-

3].X.D.1). The combination is entirely justified since an advantage (motivation) can be achieved from the prior art combination (Whelan and Meier).

The Whelan prior art discloses the verification of discovery information. (see Whelan paragraph [0049], lines 1-14: mobile unit initiates an association process to an access point; based on identification (ESSID); client invokes the correct set of association lists; mobile unit authenticates the access point; paragraph [0123], lines 3-7: client sends information (ESSID, BSSID); determine which access point mobile unit should association with)

The Whelan and Meier prior art combination discloses the claim limitations of the verification of discovery information and the verification of identification information by a transfer of identification information to the access point for verification. (see Meier col. 3, lines 1-5; col. 3, lines 15-18: send message to access point including SSID (security object); verifying the access point); verification procedure for access point)

In addition, the Whelan prior art is concerned with the concept of spoofing (see remarks Page 11) a connection. Spoofing a connection is a concern of the Whelan prior art even though the claimed invention does not mention the term but the specification does mention the spoofing concept. (see Whelan paragraph [0084], lines 1-7: to prevent spoofing attacks by foreign access points, the mobile unit will authenticate any access points it associates with)

After initial authentication, the list is utilized. But, the access point is still authenticated. (see Whelan paragraph [0052], lines 1-12: access point is still authenticated; even if access point is not on a list)

The examiner has considered the applicant's remarks concerning network devices accessing a communications network and engaging in secure associations with one or more network access points upon authenticating the access points and upon verifying the discovery information that is broadcast by the access point. Once a secure association is created, management frames transmitted between the network devices and the access points are used to control the secure association and are also verified to further enhance the security of the communications network. Applicant's arguments have thus been fully analyzed and considered but they are not persuasive.

Claim Rejections - 35 USC § 101

4. The 101 rejection has been withdrawn due to claim amendments.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims **1 - 28, 41, 42** are rejected under 35 U.S.C. 103 (a) as being unpatentable over **Whelan et al.** (US PGPUB No. **20040198220**) in view of **Meier et al.** (US Patent

No. **6,950,628**).

With Regards to Claims 1, 10, Whelan discloses in a station, computer program product comprising one or more computer-readable storage media storing computer-executable instructions that is capable of communicating with at least one access point in a communications network, a method for creating a secure association between the station and at least one access point, the method comprising:

a) obtaining discovery information from one or more access points in the communications network, the discovery information reflecting capabilities of the one or more respective access points to facilitate communication with the station; (see Whelan paragraph [0049], lines 1-10: detect (discover) information obtained from access points; col. 2, lines 30-32: software; computer readable implementation)

b) selecting one of the access points to become associated with; (see Whelan paragraph [0049], lines 10-12: placed on associated list)

c) authenticating the selected access point; (see Whelan paragraph [0054], lines 1-4; paragraph [0026], lines 1-4: authenticate access point (mobile device))

Whelan discloses the discovery of an access point (see Whelan paragraph [0013], lines 3-7: request for verification; paragraph [0009], lines 1-3; paragraph [0054], lines 1-4: authenticate access point; paragraph [0013], lines 7-10: receive response) and wherein the discovery verification request includes at least part of the discovery information obtained from the access point. (see Whelan paragraph [0049], lines 1-

14: mobile unit initiates an association process to an access point; based on identification (ESSID); client invokes the correct set of association lists; mobile unit authenticates the access point; paragraph [0123], lines 3-7: client sends information (ESSID, BSSID); determine which access point mobile unit should be associated with) Whelan does not specifically disclose a method to verify the information concerning an access point.

However, Meier discloses:

d) sending a discovery verification request to the selected access point for the discovery information of the selected access points to be verified. (see Meier col. 3, lines 1-5; col. 3, lines 15-18: send message to access point including SSID (security object); verifying the access point); verification procedure for access point)

e) receiving an acknowledgement receipt from the selected access point verifying the discovery information. (see Meier col. 6, lines 30-39: allow connection if the access point does have a matching SSID; connection is allowed (acknowledgement))

It would have been obvious to one of ordinary skill in the art to modify Whelan to use a discovery verification request as taught by Meier. One of ordinary skill in the art would have been motivated to employ the teachings of Meier in order to differentiate network access for different classes of users, especially wireless LAN users. (see Meier col. 1, lines 19-24: *" … he present invention relates generally to network access and more particularly to a method and system to differentiate* *network access for different classes of users. It is becoming increasingly important to differentiate network access for different classes of users, in particular different classes of wireless LAN users. … "*)

With Regards to Claims 2, 11, Whelan discloses a method, computer program product as recited in claims 1, 10, wherein the discovery verification request includes an identifiable security object obtained during authentication. (see Whelan paragraph [0013], lines 3-7: authentication request; paragraph [0076], lines 1-3: certificate, security object) However, Meier discloses wherein discovery verification request includes a security object. (see Meier col. 3, lines 1-5; col. 3, lines 15-18: send message to access point including SSID (security object); verifying the access point); SSID security object in verification request)

It would have been obvious to one of ordinary skill in the art to modify Whelan to use a security object in a discovery verification request as taught by Meier. One of ordinary skill in the art would have been motivated to employ the teachings of Meier in order to differentiate network access for different classes of users, especially wireless LAN users. (see Meier col. 1, lines 19-24)

With Regards to Claims 3, 12, Whelan discloses a method, computer program product as recited in claims 2, 11, wherein the identifiable security object includes at least one of an encryption key, a certificate and a hash number. (see Whelan paragraph [0076], lines 1-3: certificate, security object)

With Regards to Claims 4, 13, Whelan discloses a method, computer program product as recited in claims 1, 10, wherein authenticating the access point includes identifying a certificate from a trusted certificate authority. (see Whelan paragraph [0096], lines 1-3; paragraph [0076], lines 3-5: certificate authority (CA) utilized for authentication)

With Regards to Claims 5, 14, Whelan discloses a method, computer program product as recited in claims 4, 13, wherein the trusted certificate authority is a server of the communications network. (see Whelan paragraph [00076], lines 3-5: CA is a server)

With Regards to Claims 6, 15, Whelan discloses a method, computer program product as recited in claims 1, 10, wherein authenticating the access point is part of a mutual authentication that also involves the access point authenticating the station. (see Whelan paragraph [0009], lines 1-3; paragraph [0054], lines 1-4: mutual authentication)

With Regards to Claims 7, 16, Whelan discloses a method, computer program product as recited in claims 1, 10, further including an act of sending a frame to the access point after receiving the acknowledgment receipt, wherein the frame includes a verifiable key that indicates to the access point that the frame is actually received from the station. (see Whelan paragraph [0094], lines 1-3: shared secret key utilized to exchange messages)

With Regards to Claims 8, 17, Whelan discloses a method, computer program product as recited in claim 7, wherein the frame includes a management frame configured to control the secure association between the access point and the station. (see Whelan paragraph [0094], lines 1-3: secure exchange of messages between mobile units (access point and station))

With Regards to Claims 9, 18, Whelan discloses a method, computer program product as recited in claims 8, 16, wherein the management frame is configured to terminate the secure association. (see Whelan paragraph [0030], lines 1-5; paragraph [0030], lines 17-20: excluded list (terminate association))

With Regards to Claims 19, 24, Whelan discloses in an access point that is capable of communicating with at least one station in a communications network, a method, computer program product comprising one or more computer-readable storage media storing computer-executable instructions for creating a secure association between the station and at least one access point, the method comprising:

a) providing discovery information to the station, the discovery information reflecting capabilities of the access point to facilitate communication with the station; (see Whelan paragraph [0049], lines 1-10: provide (discovery) information obtained from access points)

b) providing a certificate with the discovery information that is used by the station to authenticate the access point; (see Whelan paragraph [0096], lines 1-3:

certificate utilized in authentication)

Whelan discloses the discovery of an access point. (see Whelan paragraph [0013], lines 3-7: request for verification; paragraph [0009], lines 1-3; paragraph [0054], lines 1-4: authenticate access point; paragraph [0013], lines 7-10: response to request) and wherein the discovery verification request includes at least part of the discovery information obtained from the access point (see Whelan paragraph [0049], lines 1-14: mobile unit initiates an association process to an access point; based on identification (ESSID); client invokes the correct set of association lists; mobile unit authenticates the access point; paragraph [0123], lines 3-7: client sends information (ESSID, BSSID); determine which access point mobile unit should be associated with) and sending an acknowledgement receipt to the station. (see Whelan paragraph [0123], lines 7-9: association information (acknowledgement) is transmitted to client over a secure connection) Whelan does not specifically disclose a method to verify the information concerning an access point.

However, Meier discloses:

c) receiving a discovery verification request from the station for the discovery information to be verified; (see Meier col. 3, lines 1-5; col. 3, lines 15-18: send message to access point including SSID (security object); verifying the access point); verification procedure for access point)

d) verifying the discovery verification request to the station. (see Meier col. 6, lines 30-39: allow connection if the access point does have a matching SSID; connection is allowed (acknowledgement))

It would have been obvious to one of ordinary skill in the art to modify Whelan to use a discovery verification request as taught by Meier. One of ordinary skill in the art would have been motivated to employ the teachings of Meier in order to differentiate network access for different classes of users, especially wireless LAN users. (see Meier col. 1, lines 19-24)

With Regards to Claims 20, 25, Whelan discloses a method, computer program product as recited in claims 19, 24, wherein the discovery verification request includes an identifiable security object obtained during authentication of the access point by the station. (see Whelan paragraph [0076], lines 3-5; paragraph [0096], lines 1-3: certificate, security object)

With Regards to Claims 21, 26, Whelan discloses a method, computer program product as recited in claims 20, 25, wherein the identifiable security object includes at least one of an encryption key, a certificate and a hash number. (see Whelan paragraph [0076], lines 3-5; paragraph [0096], lines 1-3: security object, certificate)

With Regards to Claims 22, 27, Whelan discloses a method, computer program product as recited in claims 19, 24, wherein the certificate is signed by a server of the communications network. (see Whelan paragraph [0096], lines 1-3: CA, server system, certificate signed by CA)

With Regards to Claims 23, 28, Whelan discloses a method, computer program product as recited in claims 19, 24, further including an act of authenticating the station as an authorized network device. (see Whelan paragraph [0009], lines 1-3; paragraph [0054], lines 1-4: authentication, mobile unit)

With Regards to Claim 41, Whelan discloses in a station that is capable of communicating with at least one access point in a communications network, a method for creating a secure association between the station and at least one access point, the method comprising:

a) obtaining discovery information from one or more access points in the communications network, the discovery information reflecting capabilities of the one or more respective access points to facilitate communication with the station; (see Whelan paragraph [0049], lines 1-10: detect (discover) information obtained from access points)

b) selecting one of the access points to become associated with and identifying discovery information associated therewith; (see Whelan paragraph [0049], lines 10-12: placed on associated list)

c) authenticating the selected access point by identifying a certificate associated with the discovery information, the certificate being signed by a trusted source, and receiving an identifiable security object indicating successful authentication; (see Whelan paragraph [0054], lines 1-4; paragraph [0026], lines 1-4: authenticate access point (mobile device); paragraph [0123], lines 7-9:

association information (acknowledgement) is transmitted to client over a secure connection; paragraph [0096], lines 1-3: external certificate authority possibly using PKI techniques; paragraph [0076], lines 1-8: security server can used external certificate authority (trusted third party); implies CA certificate is signed and utilized for CA authentication; security information (including discovered information) is a PKI certificate; implies signature utilized for authentication)

Whelan discloses the discovery of an access point. (see Whelan paragraph [0013], lines 3-7: request for verification; paragraph [0009], lines 1-3; paragraph [0054], lines 1-4: authenticate access point; paragraph [0013], lines 7-10: receive response) and obtained from the selected access point. (see Whelan paragraph [0049], lines 1-14: mobile unit initiates an association process to an access point; based on identification (ESSID); client invokes the correct set of association lists; mobile unit authenticates the access point; paragraph [0123], lines 3-7: client sends information (ESSID, BSSID); determine which access point mobile unit should be associated with) Whelan does not specifically disclose a method to verify the information concerning an access point.

However, Meier discloses:

validating the selected access point discovery information by:

d) sending a discovery verification request to the selected access point, wherein the discovery verification request includes at least a part of the discovery information, the identifiable security object, or both, (see Meier col. 3, lines 1-5; col. 3, lines 15-18: send message to access point including SSID (security object); verifying the access point); verification procedure for access point)

e) receiving an acknowledgement receipt from the selected access point verifying the discovery information, wherein if verified the acknowledgement receipt includes the security object or a derivative thereof. (see Meier col. 6, lines 30-39: allow connection if the access point does have a matching SSID; connection is allowed (acknowledgement))

It would have been obvious to one of ordinary skill in the art to modify Whelan to use a discovery verification request as taught by Meier. One of ordinary skill in the art would have been motivated to employ the teachings of Meier in order to differentiate network access for different classes of users, especially wireless LAN users. (see Meier col. 1, lines 19-24)

With Regards to Claim 42, Whelan discloses a method as recited in claim 41, wherein the identifiable security object includes at least one of an encryption key, a certificate and a hash number. (see Whelan paragraph [0076], lines 1-3: certificate, security object)

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436

Carlton V. Johnson
Examiner
Art Unit 2436

CVJ
January 21, 2009